Pergamon

Acta Astronautica Vol. 43, Nos. 3–6, pp. 211–222, 1998

Printed in Great Britain
PII: S0094-5765(98)00155-6
0094-5765/98/$—see front matter

STRUCTURED METHODS FOR IDENTIFYING AND CORRECTING POTENTIAL HUMAN ERRORS IN SPACE OPERATIONS

William R. Nelson, Lon N. Haney, Lee T. Ostrom, and Robert E. Richards
Idaho National Engineering and Environmental Laboratory
Lockheed Martin Idaho Technologies
P.O. Box 1625, Idaho Falls ID, 83415-3855 USA
wnr@inel.gov
Fax: (208) 526-2930

Abstract

Human performance plays a significant role in the development and operation of any complex system, and human errors are significant contributors to degraded performance, incidents, and accidents for technologies as diverse as medical systems, commercial aircraft, offshore oil platforms, nuclear power plants, and space systems. To date, serious accidents attributed to human error have fortunately been rare in space operations. However, as flight rates go up and the duration of space missions increases, the accident rate could increase unless proactive action is taken to identify and correct potential human errors in space operations. The Idaho National Engineering and Environmental Laboratory (INEEL) has developed and applied structured methods of human error analysis to identify potential human errors, assess their effects on system performance, and develop strategies to prevent the errors or mitigate their consequences. These methods are being applied in NASA-sponsored programs to the domain of commercial aviation, focusing on airplane maintenance and air traffic management. The application of human error analysis to space operations could contribute to minimize the risks associated with human error in the design and operation of future space systems.

1. INTRODUCTION

Near and long term space operations will be highly dependent on human participation to ensure their success. Along with their significant capabilities to perform space operations and to diagnose and correct malfunctions when they occur, humans also have a built-in propensity to commit errors. Human errors have been identified as the source of at least 60% of the incidents and errors that occur in commercial aviation. It can be assumed that large numbers of human errors occur in space operations as well, even though in most cases the redundancies and diversities built into the design of space systems prevent the errors from leading to serious consequences. To date rigorous design practices, quality control, and relatively low flight rates have minimized the occurrence of serious accidents resulting from human error. However, as flight rates increase in the future, accidents attributed to human error are likely to increase unless error frequencies can be reduced. In addition, when it is acknowledged that many system failures (such as the Challenger accident) have their roots in human errors that occur in the design phase, it becomes apparent that the identification and elimination of potential human errors could significantly decrease the risks of space operations. This will become critical during the design of more complex and longer term missions such as the International Space Station and manned missions to Mars.

2. BACKGROUND

The Idaho National Engineering and Environmental Laboratory (INEEL) has worked for many years to develop and apply structured methods to identify and correct potential human errors. This work was initiated to support Probabilistic Risk Assessment (PRA) for the nuclear power industry. Methods of Human Reliability Analysis (HRA) have been adapted and extended so that potential human errors can be identified, their consequences in conjunction with other human errors and hardware failures can be assessed, and their relative contribution to overall system risk can be calculated. These methods have reached a state of maturity and acceptance in the commercial nuclear power industry.

During the last few years we have focused on adapting these methods to enhance their applicability as practical tools for system design, and to test their application to domains outside of nuclear power. Since 1994 we have performed research under the NASA Advanced Concepts Program in partnership with NASA Ames Research Center and Boeing Commercial Airplane Group to develop methods and tools to apply human error analysis to the design of commercial transport aircraft. During the course of this program we have tested the applicability of human error analysis methods for application to maintenance tasks for commercial aviation. Based on this experience we have developed a framework and methodology called FRANCIE (Framework Assessing Notorious Contributing Influences for Error) that facilitates identification and modeling of important human errors and the factors that influence those errors. We have also developed a software tool called THEA (Tool for Human Error Analysis) for use by airplane procedure developers and maintenance engineers. The tool is a structured approach incorporating FRANCIE for analyzing maintenance tasks for the purpose of identifying potential errors, performance shaping factors that can influence errors, and potential design or procedure changes that could reduce the likelihood for errors. The software has undergone preliminary testing by NASA and Boeing and is currently available for release to the commercial aviation industry in prototype form.

We believe that our structured methods for human error analysis and our prototype software tool could be adapted for application to reduce the potential for human error in space operations. We are currently exploring opportunities to test the methods and tools for ground processing operations. If such an application proves successful, the methods could be adapted and applied to space operations such as the Space Shuttle, Space Station, or other manned or unmanned space missions. We believe that such tools could contribute to minimize the potential for human errors in the design and operation of future space systems.

3. CHARACTERISTICS OF HUMAN ERRORS IN SPACE OPERATIONS

The types of errors that can occur in space operations are very similar to those that are associated with any complex technical activity such as commercial aviation. Human errors have the potential to occur in all phases of space operation including errors in design, analysis, maintenance, ground processing, launch decision making, and flight operations. Some of the types of errors that could occur include calculation errors, failure to identify operational conditions or scenarios, manual manipulation errors, selection of incorrect components, incorrect assessment of operational conditions, or selection of an incorrect response for a malfunction situation. While many human engineering efforts associated with the space program have focused on flight operations, we believe that it is equally important to address human errors that could occur in other phases of space operations as well. In fact, the greatest leverage for human error analysis will be to identify and eliminate those errors that occur during design, since a large fraction of operational errors have their direct roots in the failure of the designer to consider some factor concerning system operations.

Certain conditions associated with task performance may have a direct influence on the likelihood that an error might occur. These are referred to as Performance Shaping Factors (PSFs). PSFs that might contribute to the occurrence of errors in space operations include environmental factors (light, temperature, noise, etc.), procedure quality, quality of the human-machine interface, time available, organizational factors, and stress.

4. METHODS FOR HUMAN ERROR ANALYSIS

The methods for human error analysis that we have developed at INEEL have their roots in human reliability analysis methods developed for performing risk assessment in the nuclear industry. Human error analysis, for the purposes of this paper, is the systematic identification and modeling of potential human errors in the design, construction, operation, or maintenance of a technical system. Major reviews and summaries of the issues surrounding the qualitative and quantitative aspects of human error analysis can be found in Dougherty and Fragola [1], Gertman and Blackman [2], Haney et al. [3], and Reason [4]. A number of modeling techniques can be used to characterize human errors, and place them in the context of other errors and hardware failures that can combine to lead to undesirable consequences. System analysis and functional modeling using functional analysis trees are used to help identify potential human errors and tasks that may degrade or fail systems. Human reliability analysis event trees are used to represent sequences of human errors (failure paths) that result in the failure of a task as well as to represent the success path and possible recovery paths for the task. These tools are used to model the interactions of human tasks and hardware systems, and to identify single errors or combinations of human errors and hardware failures that may lead to degraded system performance.

The specific methods and tools that we have developed to apply human error analysis to commercial aviation are briefly summarized in the following sections.

4.1 *FRANCIE*

The Framework Assessing Notorious Contributing Influences for Error (FRANCIE) is a framework and methodology that facilitates identification and modeling of important human errors and the factors that influence those errors. FRANCIE also provides information and methods to guide the development of strategies for reducing the probability of human error. FRANCIE is designed to be proactive as well as reactive. It is proactive by allowing error analysis of existing systems, or by being implemented as part of the design phase to assess and reduce potential error related to design issues. It is reactive by allowing error analysis of events, or serving as a tool to guide and facilitate incident investigation. The framework structure and methodology can be applied to any domain given development of the appropriate error type and performance shaping factor taxonomy. The first FRANCIE taxonomy developed is for airplane maintenance.

FRANCIE is designed to provide a graded approach for error analysis producing useful results at each stage. FRANCIE provides the capability of performing simple qualitative analyses (e.g. identifying potential errors and their influences), more detailed qualitative analyses (e.g. modeling task structure, recovery, dependencies, etc.), or detailed quantitative analyses (e.g. estimates of human error probabilities, error chain probabilities, etc.). The framework and methodology allows performance of sensitivity analyses to support decision making in terms of design or procedural alternatives relative to human error potential. FRANCIE is designed for use by system designers, procedure writers, operations or maintenance personnel, reliability analysts, or anyone interested in analyzing human error for a simple or complex system.

4.2 *THEA*

The Tool for Human Error Analysis (THEA), was created to:

- Enable an individual who is expert with his or her work, but not necessarily with the concepts and techniques of human error and reliability analysis, to proficiently perform human error analyses of tasks within his or her work area.

- Enable a novice to obtain useful qualitative and, optionally, quantitative results within a few hours of initial use and with a minimum amount of formal instruction and consulting support.

- Assist a user in exploring the potential impact that initial error events and failures to recover from those error events can have on an overall task performance.

- Assist a user in identifying and assessing the key PSFs that contribute to human error in a given situation and for a given task.

Additionally, THEA was designed to be easily adaptable to wide a variety of potential implementation domains (e.g. transportation, chemical processing, food processing, and operations).

THEA utilizes the FRANCIE framework and methodology to facilitate human error analysis. Although THEA 1.0 utilizes primarily the FRANCIE methodology, it has been designed to be capable of supporting numerous human error and human reliability analysis methods. For example, only minor changes to a few forms and calculations would be needed to support complete quantitative human reliability analyses. Other tools supporting other analysis methodologies will be added as time and needs dictate. THEA also supports the most common qualitative models, as well as a hybrid quantification method that combines several well-accepted human reliability quantification methods.

5. APPLICATIONS OF HUMAN ERROR ANALYSIS TO AVIATION

Our primary applications of human error analysis to date have been for commercial and military aviation. These efforts are briefly described in the following.

Our first application of human error analysis to aviation was to evaluate pilot problem solving and situation awareness for equipment malfunction and air combat scenarios [5]. A series of experimental studies was performed for the U.S. Air Force to test the suitability of the approach to assess complex human performance. Functional models of pilot performance were developed for the tasks of interest. Actual performance in the simulator was then observed and the behaviors observed were mapped onto the functional models. These studies showed that models of human tasks could be used to assess the performance of pilots in actual task performance in the simulator.

Our next application was to assess the effects of cockpit automation on pilot performance in glass cockpit aircraft. This study, funded by NASA, had the objective to determine whether cockpit automation influences the occurrence of errors in altitude maintenance. Reports from the Aviation Safety Reporting System (ASRS) representing 200 altitude deviation events were reviewed. Models of the tasks required for altitude maintenance were developed, and the specific details of each event were mapped onto the models. The errors were then categorized across the events that were analyzed to extract the common factors leading to altitude deviations. This study highlighted the applicability of the task modeling structures for categorizing the factors that lead to human errors in flight operations. Details regarding this study are found in Nelson et al., [6].

Our most recent activity to apply human error analysis to aviation has been the Structured Human Error Analysis for Aircraft Design program. This program was conducted in partnership with the NASA Ames Research Center and Boeing Commercial Airplane Group under the sponsorship of the NASA Advanced Concepts Program. The objectives of the program were to test the applicability of human error analysis to airplane design, and to develop methods and tools to identify and correct human errors, focusing on airplane maintenance. Airplane maintenance tasks were analyzed using human error analysis, and the results were compared to operational experience to verify the validity of the analysis. As described above, a human error framework (FRANCIE) and a prototype software tool (THEA) were developed to allow the performance of human error analysis by procedure developers and maintenance engineers. In addition, data on human error were collected for selected maintenance tasks for military aircraft, and expert opinion was utilized to assess the contributions of the various performance shaping factors to the occurrence of different error types. This project has demonstrated that human error analysis can be used to identify potential human error in aviation operations, and that strategies for preventing errors or reducing their consequences can be systematically determined.

6. INTEGRATED DESIGN ENVIRONMENT FOR HUMAN RELIABILITY ANALYSIS

Human factors research at the Idaho National Engineering and Environmental Laboratory over the last few years has focused on the development of an effective framework to apply human performance and human reliability methods to the full system development cycle, so that the full effectiveness of the methods to enhance design quality and system performance can be realized. We believe that the maximum leverage of human factors methods is obtained when applied as early as possible in system development, for example during the identification of requirements and during the process of system design. Also, we believe that human performance and human reliability methods can be applied to engineering processes as well as to the operation and maintenance of the resulting system. For example, system design is a human activity just as much as is operation, so human performance and reliability in performing design tasks can be evaluated using the same methods. We also believe that system design should rely to the greatest degree possible on the lessons learned from operational experience, so that design mistakes of the past are not repeated. Finally, we believe that human performance and human reliability methods should be directly integrated with the engineering processes and program management activities involved in system development, rather than functioning as an add-on to the system development process. The methods and framework developed can serve as a common language for communication among engineers, designers, human factors personnel, risk management experts, and program management.

The work described above has been pursued in programs in a wide variety of technical domains, beginning with nuclear power plant operations. Since the mid-1980's we have transferred the methods and tools developed in the nuclear domain to military weapons systems and aircraft, offshore oil and shipping operations, and commercial aviation operations and aircraft design. Through these diverse applications we have developed an integrated design environment for application of human performance analysis, human reliability analysis, operational data analysis, and simulation studies of human performance to the design and development of complex systems. We are currently working to apply this framework to the development of advanced air traffic management systems as part of NASA's Advanced Air Transportation Technologies (AATT) program.

Fig. 1 illustrates the main features of the integrated design environment for human performance and human reliability analysis that is under development at INEEL. The framework is comprised of five major elements:

- Lessons learned
- Functional analysis
- Simulation
- Human performance and human error analysis
- Design engineering tools

Each of these elements is described in greater detail in the following sections.

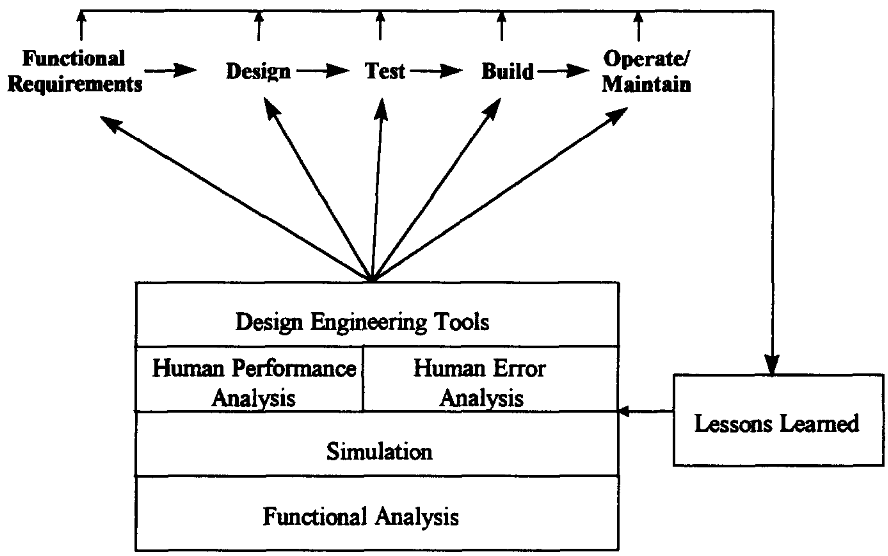

Fig. 1. Integrated Design Environment for Human Performance and Human Reliability Analysis

6.1. Lessons Learned

The effective extraction of lessons learned from operational experience is a key factor in the development of quality designs for complex systems. Much operational data analysis focuses on statistical analysis of key parameters associated with a class of accidents and incidents. However, it is difficult to extract usable design guidance from such quantitative analyses. Rather, we believe that it is important to extract qualitative, contextual information from operational experience so that lessons can be learned about the influences that lead to human error and to guide designs to eliminate to the degree possible those error inducing situations. To this end, we have developed and applied analytic methods that can be used to interpret operational data to extract qualitative lessons learned across a range of events. We have applied these methods to the evaluation of incidents in nuclear power plants, offshore oil operations, nuclear medicine, marine casualties, and commercial aviation.

6.2 Functional Analysis

An important foundation of system development is functional analysis. Functional analysis is used to identify those critical functions related to safety, production, economics, etc. that must be optimized during design and maintained during operation to ensure that system objectives are achieved. The functional analysis approach that we have developed at INEEL is based on the systematic identification of critical functions, the tasks (human, hardware, and software) that are performed to maintain them, the resources that can be utilized to maintain the functions, and the support systems that are required for the operation of the resources. Once a functional model is developed, it can be used to identify system vulnerabilities to single or combined component and human failures, explore the performance of the system in response to any number of operational scenarios, explore various design alternatives from a functional perspective, or assess human performance in simulation or operational tests. In addition, a functional model can serve as the basis for procedures or computerized operator support systems, particularly to guide critical function maintenance during off-normal conditions.

6.3 Simulation

Simulation of course can play an important role in helping incorporate human performance and human reliability knowledge into system design. Various design alternatives can be tested in the simulation laboratory to investigate the advantages and disadvantages of various design features relative to human performance and reliability. Simulation is particularly effective when it is integrated into the total design environment, so that the insights gained from operational data analysis and human reliability evaluations can be used to identify what information is required from a simulation study and to assist the experimental design. Simulation is used most effectively when it is an integral part of the design-test-modify process rather than simply a "laboratory" for major experiments where "statistically significant differences" are sought to support a theoretical hypothesis regarding human behavior. Rather, simulation should be viewed as a powerful tool with which to try out various design alternatives in a tightly-coupled feedback loop to investigate design options.

6.4 Human Performance and Human Error Analysis

Other key components of the INEEL integrated design environment include structured methods for human performance analysis and human error analysis. These methods can be used to systematically evaluate system design features and assess their suitability when compared with functional or reliability objectives for overall system performance. As discussed earlier in this paper, human error analysis can be used to help identify potential human errors, how they interact with other errors and component failures to lead to serious consequences, and potential strategies to prevent or mitigate the consequences of specific errors.

6.5 Design Engineering Tools

The final element of the INEEL integrated design environment for human performance and human reliability analysis is a set of design engineering tools. These tools, currently under development, allow the systematic application of the other elements of the design environment in the system development process. As illustrated in Fig. 1, these tools will allow the results of analyses to be applied at all phases of system development.

Different tools will be appropriate for different stages in the process. For example, functional analysis tools can be used very early in the development process, before any design details are available. Even at this stage, systematic identification and evaluation of the critical functions and possible task structures will allow a systematic assessment of system vulnerabilities to functional failures, and to support the development of design requirements that will optimize system design from the functional perspective. Later in the process when design details become available, human reliability analysis and human error analysis can be called upon to perform detailed assessments of different design options.

7. POTENTIAL APPLICATIONS TO SPACE OPERATIONS

The structured methods of human error analysis described in this paper, as well as the integrated design environment for human performance and human reliability analysis currently under development, have many potential applications as part of a systematic program to reduce human errors in space operations. For example, the methods and tools could be used to improve the design of equipment and procedures to minimize the likelihood of human errors, in essentially the same manner they have been applied to aviation operations. One of the most straightforward applications would be for the reduction of human errors in ground processing. The tasks associated with spacecraft ground processing have a lot of similarities with maintenance tasks for commercial aircraft, so the FRANCIE structure developed for aviation could be utilized with only minor modifications. Such an application would provide a straightforward test to assess the applicability of the methods we have developed to space operations tasks.

FRANCIE and THEA were developed in a generic and modular form, so it would be straightforward to adapt them to other task domains, for example to assess the tasks associated with on-orbit operations for the Space Shuttle or Space Station. By encoding expert knowledge and experience regarding task performance in the weightless environment, it would be possible to review existing designs and procedures with a view to reduce human errors, and to develop new equipment designs and task structures so that human reliability considerations can be taken into consideration from the very beginning.

A more ambitious undertaking would be to apply the integrated design environment to enhance the overall system design, development, test, and evaluation (DDT&E) process to minimize the occurrence and consequences of human errors that might occur at any stage of system development. This would take advantage of the maximum leverage of l uman error analysis, by proactively examining the entire system development process for opportunities to reduce error. For example, such an approach could highlight situations where errors in design could result in equipment or procedures that could increase the likelihood of serious incidents in actual operations. Strategies for reducing these errors could then be developed, thereby increasing the overall quality of the design process itself. Our ongoing application of the integrated design environment to the development of air traffic management systems within NASA's Advanced Air Transportation Technologies program could serve as a model for such an application to space programs. Such a comprehensive application of the integrated design environment would be most suitable for a program that is still early in the requirements definition stage, for example proposed manned missions to Mars.

Up until the present, worldwide space programs have fortunately experienced only a very few serious incidents and accidents that could be traced to human error. This record is a tribute to the stringent safety policies associated with space programs and the dedication and vigilance of the personnel involved. However, as mission frequency, complexity, and duration increase, and reduced space budgets place increased demand on program and support personnel, the frequency of events attributable to human error is bound to increase unless proactive action is taken. Structured methods of human error analysis such as those described in this paper could help maintain and improve the excellent safety record that has allowed international space programs to achieve such incredible accomplishments over the last four decades.

8. ACKNOWLEDGMENTS

Work supported by the National Aeronautics and Space Administration, under DOE Idaho Operations Office Contract DE-AC07-94ID13223.

9. REFERENCES

1. Dougherty, E.M. Jr., and Fragola, J.R. (1988), Human Reliability Analysis, a Systems Engineering Approach with Nuclear Power Plant Applications, John Wiley, New York.

2. Gertman, D.I., and Blackman, H.S. (1993), A Summary of Data and Methods for Human Reliability and Safety Analysis, John Wiley Interscience, New York.

3. Haney, L.N., Blackman, H.S., Bell, B.J., Rose, S.E., Hesse, D.J., Minton, L.A., and Jenkins, J.P. (1989), Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Methods Integration and Evaluation Program (RMIEP), U.S. Nuclear Regulatory Commission, Washington, D.C., NUREG/CR-4835.

4. Reason, James. (1990), Human Error, Cambridge University Press, Cambridge.

5. Blackman, H.S., Hahn, H.A., and Nelson, W.R. (1992), "Complex Human Performance Measurement in an Aviation Environment," Human Performance, Vol. 5, No. 4, 1992.

6. Nelson, W.R., Byers, J.C., Haney, L.N., Ostrom, L.T., and Reece, W.J. (1993), "Lessons Learned from Pilot Errors Using Automated Systems in Advanced Technology Aircraft." *Proceedings of American Nuclear Society Topical Meeting on Nuclear Power Plant Instrumentation, Control, and Man-Machine Interface Technologies,* Oak Ridge, TN.